GR-33 Privacy for MPEG-DASH Based Video Streaming

Abstract

MPEG-DASH is a video streaming standard that outlines protocols for sending audio and video content from a server to a client over HTTP. However, it creates an opportunity for an adversary to invade users' privacy. Once a fingerprint is created, the adversary can use this to identify whether a target user is watching the corresponding video. We propose a defense against the attack with rigorous privacy and performance constraints, creating a totally private, scalable solution that outperforms the extant schemes. Our algorithm, No Data are Alone (NDA), is based on K-Means clustering. The experimental results show that our scheme is more than two times as efficient as others. Additionally, no classifier can achieve an accuracy above 7% against videos obfuscated with our scheme.

Introduction

One of the components of MPEG-DASH that allows it to become an effective attack surface is the reliance on variable bit-rate encoding (VBR). Bit-rate is the amount of bits needed to encode one second of video that is sent from server to client. VBR only sends as many bits as needed to render each segment of video, because of this, a unique fingerprint can be made for a video.

The most effective attack based on this information uses a Convolutional Neural Network to classify the video title. This classifier had an accuracy above 95% for YouTube videos. Meaning an adversary can predict which video a user is watching with 95% accuracy.

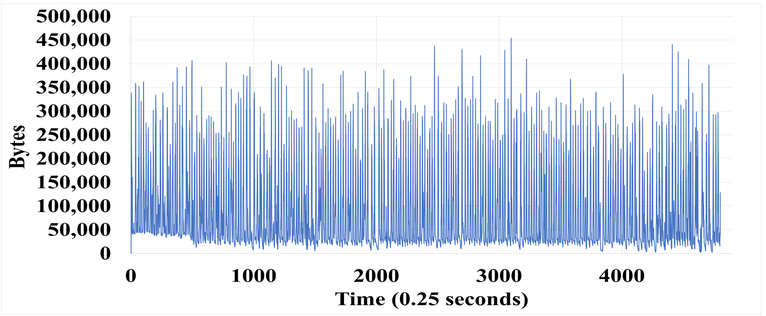
We create a defense using K-Means clustering. K-Means clustering is an unsupervised learning algorithm that puts data similar data into groups, then calculates the average of the data in each group. There is an average for every group of data.

Research Question(s)

The video streaming industry is large, and video streaming is computationally expensive, meaning it requires lots of resources from a computer. Therefore, the main question is not only how to defend against this attack, but how can we create a defense that maintains efficiency?

Materials and Methods

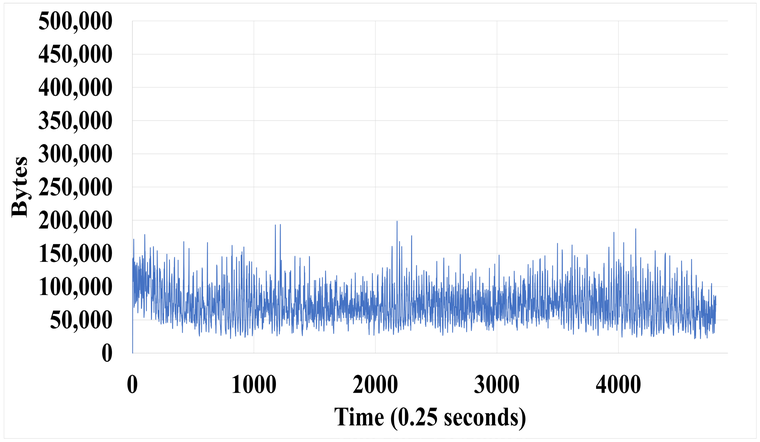
We recorded data from 40 YouTube videos 100 times each, giving us 4000 data points to use. A graphical representation of a video recording is shown below.



Using this data, we trained a Convolutional Neural Network, to recreate the attack so that we could test our defense scheme. We then used our own algorithm, based on K-Means clustering, to create a new video request pattern so that an adversary couldn't recognize the video being watched by the user. We created the new video pattern (an alteration of the graph above) by grouping similar videos together, then taking the average of all the similar videos. This average then functioned as the new video request pattern. We then tested the attack against our defense and measured the efficiency of our defense against the original request pattern.

Results

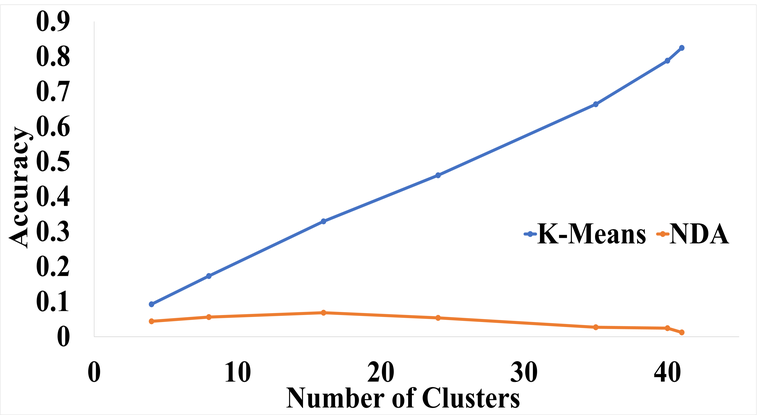
The result of our defensive scheme can be seen in the graph below. This graph is an altered (private) version of the graph shown in the previous section, Materials and Methods.



Once we had our defensive scheme created, we tested the attack against it. When testing the attack against our scheme, the attack never reached an accuracy level above 7% when previously it had an attack accuracy of 95% before we implemented our defense scheme.

We based our algorithm on K-Means clustering. K-Means clustering assigns data points to a group, then computes the average for each group. We altered the algorithm because traditional K-Means will leave data points alone in their own group. These alone videos aren't private, because the average of that group would be the same as the only data point in that group, and we used the average to create a new video pattern.

To overcome the problem of having data along in a group, we reassigned video so that no data points are alone in a group (cluster). This group reassignment was not random, we calculate which group reassignment would give the best computational efficiency and reassign based on this. Below shows why our alteration is necessary. As the number of groups (clusters) of data increases, there are more data points alone in a group, and therefore the attack accuracy will increase to a point where it is no longer private. In this graph, a value of 0.9 represents an attack accuracy of 90%.



Conclusions

This work aimed to develop a privacy preservation scheme that conformed to rigorous privacy standards while having a high computational efficiency, overcoming the common trade-off between privacy and computational speed. We asserted that unless a defense scheme lowered the attack method accuracy below 10%, it was not fully private. Using K-Means clustering as a base, we created our own algorithm, No Data Are Alone, that accomplished this goal. Our algorithm provided privacy at a higher level when measures against the most robust attack methods, which relied on a Convolutional Neural Network (CNN). The attack CNN being trained on data we collected never improved in accuracy even with training on the obfuscated data and was ever able to reach an accuracy above 7%. Other differential privacy based defense techniques were vulnerable to a CNN trained against them, and the CNNs trained against these schemes had 20% or greater increases in accuracy. Additionally, the computational cost of our scheme was less than half of the best performing scheme.

Acknowledgments

First and foremost I would like to thank my advisor, Dr. Junggab Son for giving me the opportunity and resources to complete this project. I would also like to thank Dr. Jeehyeong Kim, who guided me into this project and mentored me through it. Additionally, I would like to thank my colleagues Hong Kyu and Victor, who helped me with implementation and final paper revisions.

Contact Information

My email is lcranfil@students.kennesaw.edu
Contact information for all authors can be found on our official lab website:
http://i2s.kennesaw.edu

References

[1] I. Sodagar, "The mpeg-dash standard for multimedia streaming over the internet," IEEE MultiMedia, vol. 18, no. 4, pp. 62–67, 2011.

[2] R. Schuster, V. Shmatikov, and E. Tromer, "Beauty and the burst : Remote identification of encrypted video streams," in 26th USENIX Security Symposium (USENIX Security 17), pp. 1357–1374, 2017.

[3] J. Gu, J. Wang, Z. Yu, and K. Shen, "Traffic-based side-channel attack in video streaming," IEEE/ACM Transactions on Networking, vol. 27, no. 3, pp. 972–985, 2019.

[4] A. Reed and B. Klimkowski, "Leaky streams: Identifying variable bitrate dash videos streamed over encrypted 802.11n connections," in201613th IEEE Annual Consumer Communications Networking Conference(CCNC), pp. 1107–1112, 2016.

[5] R. Dubin, A. Dvir, O. Pele, and O. Hadar, "I know what you saw lastminute—encrypted http adaptive video streaming title classification,"IEEE Transactions on Information Forensics and Security, vol. 12,no. 12, pp. 3039–3049, 2017.

[6] S. Kadloor, N. Kiyavash, and P. Venkitasubramaniam, "Mitigating timing side channel in shared schedulers," IEEE/ACM Transactions on Networking, vol. 24, no. 3, pp. 1562–1573, 2016.

[7] X. Zhang, J. Hamm, M. K. Reiter, and Y. Zhang, "Statistical privacy for streaming traffic.," in NDSS, 2019.

[8] Q. Xiao, M. K. Reiter, and Y. Zhang, "Mitigating storage side channels using statistical privacy mechanisms," in Proceedings of the 22ndACM SIGSAC Conference on Computer and Communications Security, pp. 1582–1594, 2015.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s): Luke Cranfill, Dr. Jeehyeong Kim, Hong Kyu Lee, Victor Yondum Kemmeo
Advisor(s): Dr. Junggab Son